https://doi.org/10.48009/3_iis_2019_37-46

Issues in Information Systems
Volume 20, Issue 3, pp. 37-46, 2019

SECURE PROTOCOLS AND VIRTUAL PRIVATE NETWORKS: AN EVALUATION

Raymond Angelo, Quinnipiac University, raymond.angelo @quinnipiac.edu

ABSTRACT

Network protocols are by their design insecure and open to threats from cybercriminals. Secure network protocols, such as L2TP, IPsec, TLS, and OpenVPN need to be implemented to assure confidentiality, authentication, and integrity. The advantages and disadvantages of these protocols are discussed. A preferred choice of these protocols for implementation in a virtual private network is presented in the context of the Open Systems Interconnection or Interface (OSI) Model. Secure protocols are discussed with reference to the implementation of e-commerce and the Internet of Things (IoT).

Keywords: secure protocols, security, virtual private networks, encryption, tunneling.

INTRODUCTION

For effective communication there need to be well-defined structures that describe the rules of that interchange. For computers and networks, protocols have been developed for successful and effective exchange of information (Frank, 2017). Protocols articulate the rules, syntax, and message formats that define communication exchanges (Singer & Friedman, 2014). The inventors of data communications and the Internet developed open standards so that communication would be predictable, reliable and easy. However, they could not foresee the malicious intent of cybercriminals to penetrate and steal information from network data communications (Frank, 2017; Pandey & Misra, 2016; Zhipeng et al., 2018). This has led to the development of secure protocols that enhance the safety of data exchange through networks, by using advanced techniques that will be described and evaluated in this paper (Garge & Hegde, 2011).

In order to appreciate the protocols discussed here, it is helpful and necessary to view them in the context of two landmark models. The International Standards Organization (ISO), the world's largest developer of international standards for a wide variety of products and services, developed the Open Systems Interconnection reference model. The OSI model is a layered framework for developing networking protocols, and provides a foundation for protocols to be used for the Internet and all computer hardware and software communications (Elezia & Raufia, 2015; Frank, 2017; Salman, 2017; Zhipeng et al., 2018). In addition, the TCP/IP protocol stack, which pre-dates the OSI Model, was developed to provide definition to protocols that are popular in data communications. It is characterized as protocol model because it established a hierarchical set of related protocols in a suite required to interface with humans and data networks, as well as describing the functions that occur at each layer of protocols within the suite (Frank, 2017). In contrast, the OSI Reference model is less descriptive at the protocol layers, but provides a sufficient level of detail to define precisely the services of the network architecture. Both the OSI and TCP/IP have defined the functions at the layers in a stack. The stack interaction moves encapsulated or enveloped information in the way that paper mail moves from one person to another. Encapsulation is a key concept for security, since it requires a protocol to envelope data from higher-level protocols, and provides opportunity for encryption.

Privacy of communication implies that the data transmitted on a link is readable only by the intended recipients and no one else. This is done by encrypting the transmitted message. Encryption requires keys that perform the encryption and the two end-points require that they have the right keys to encrypt as well as decrypt. Exchange of keys between the two end-points is a challenge. Many privacy schemes involve either single key (shared) or dual key cryptography. Encryption uses a complex algorithm called a cipher in order to turn normalized data (plaintext) into a series of seemingly random characters (cipher text) that is unreadable by those without a special key in which to decrypt it. Hashing may also be used to mask variable length text into a fixed length (Frank, 2017).

Security protocols address security goals, including authentication or confidentiality. They attempt to forego attacks. In particular, authentication, or logging in, enables verification of identity. Authentication is accomplished through verification of the transmitted password (Frank, 2017).

The OSI Model does a better job at detailing the functions at each layer. It is helpful to this discussion to understand the functional level of the OSI stack to appreciate the work and responsibilities toward security of the protocols at those levels. For Example, IP is a Network protocol, which means it produces a packet that contains address information between devices communicating on a network and can provide routing information between networks. In general the lower in the stack that a security protocol works, the better. This is because it is preferable for protocols to prevent access to computers on a network (Layer 3), for example, rather than at layers that deal with applications and data (Layers 4-7).

For the purposes of discussing and illustrating the roles of the secure protocols presented, we will categorize the protocols by using the OSI reference model. There are seven layers in the Reference Model: Application, Presentation, Session, Transport, Network, Data Link, and Physical. Column one represents the OSI Layer, and a brief description of the job that each layer accomplishes. Column two shows some well-known TCP/IP protocols. Column three shows the secure protocols that will be discussed in this paper.

Table 1. Map of Secure Protocols to the OSI Model

OSI Model Layer	TCP/IP Protocols	Secure Protocols
7. Application Services the end user	FTP, HTTP	
6. Presentation Data and Encryption		
5. Session Host to host communication		L2TP
4. Transport End to End reliability	TCP, UDP	TLS
3. Network Logical Addressing	IP	IPsec, OpenVPN
2. Data Link Physical Addressing		
1.Physical Media and Transmission	Ethernet, Token Passing	

Our discussion around secure protocols will center on Layers, 3 and 4, and 5 of the OSI model, as they describe, network or device addressing and communication, application port access, and encryption.

Why we need Secure Protocols

Jyothi and Reddy (2018) stated the fundamental problem with data communications by indicating that "data packets traveling the Internet are transported in clear text. Consequently, anyone who can see Internet traffic can also read the data contained in the packets (p. 920)". Elezia and Raufia (2015) indicated that the most common protocol, the Internet Protocol (IP), is not secure, since it makes all hosts on the network discoverable. The protocol does not provide confidentiality and creates opportunity for outside attacks. By being able to access the IP address of a device, hackers can potentially take control of that device, and by reading information from the TCP segment from the Transport Layer, they can reach into the application data, and steal information, such as social security numbers, credit card information, and bank account information, to name a few.

GOALS AND RESEARCH QUESTION

The goal of this research is to determine an optimal protocol for use in the protection of virtual private networks. Companies need to understand which protocols are at work in commercial security software. This question will be addressed primarily with respect to security exposure relative to the layers of the hierarchal Open Systems Interface model. As described, a protocol that acts at the lower level of the OSI model, compared to other protocols, will be preferred.

Whether in the use of secure business implementation on the internet (Mazzarol, 2015), US Army defense (Cirincione et al., 2019), data center operations for affordable backup (Lee et al., 2019), enhanced network security design (Koujalagi, 2018), or higher education (Zameer et al., 2017), virtual private network implementation will continue to grow in the internet of things. The security of these networks is as critical as its deployment.

The OSI Model recognizes the data pay loads at levels or layers of network information transmission, from physical signals to application data. Since the model is hierarchal, and at each level the data in interpreted for different information. At Layer One signals are transmitted, and no addressing is possible. At Layer Two, machine addresses are available. At Layer Three, we can identify any machine on a network or the internet. At layers above that (4-7), we are interpreting application data. As stated, we do not want to begin security defense at the higher levels, which would theoretically allow an insecure path to a machine. An important measure of security, then, is the layer at which the protocol does it work, the lower the level the better.

The following research questions was addressed in context of the goals previously described:

Research question #1: is there a preferred choice of protocols for implementation in a virtual private network as evaluated in the context of the Open Systems Interface?

VIRTUAL PRIVATE NETWORKS (VPNS)

In 2002, and again ten years later, IBM and American Express reached agreement on a multibillion dollar outsourcing deal, where American Express' web site, network servers, data storage, and help-desk support were to be (and still are) hosted in IBM facilities. To make this happen, IBM and American Express use virtual private networks to secure the exchange of confidential information, including credit card information, ongoing contract development, pricing, and other company specific financial information. Much of this work is done by hundreds of IBM and American Express employees in IBM data centers and from their homes. The technology beneath this massive system is the virtual private network ("American Express, IBM Sign", 2002; "American Express, IBM Set", 2002).

A virtual private network (VPN), and the protocols associated with it, creates a private network within a public network, such as the Internet, companies' intranets and extranets, and home offices (Jyothi & Reddy, 2018; Zhipeng et al., 2018). The technology creates a "virtual" network that traverses many physical networks and appears to the end user as one network. More importantly, applications and protocols running across the virtual network benefit from the security management that secure protocols can provide.

Prior to the turn of the century, businesses had to rely on private networks of leased lines provided by phone companies to connect geographically dispersed office and employees. This technology was expensive, costs were associated with distances and speeds. This was not practical for small business or individuals (Jyothi & Reddy, 2018; Skendzic & Kovacic, 2017). The implementation of virtual circuits, or logical, re-routable paths between source ports to the destination ports, allowed for dynamic, real time network maps, and significantly reduced costs when compared to permanent physical circuits and paths of leased lines. Today, some popular vendor VPN implementations are free of charge (Feilner, 2006; Skendzic & Kovacic, 2017). In addition, failure in a leased line will require repair before communications can be restored on those lines, whereas virtual lines can auto-reconfigure and provide uninterrupted service (Jyothi & Reddy, 2018; Northcutt et al., 2003; Vachon & Graziani, 2008).

The key to a secure VPN is to provide an encrypted tunnel through a clear text network (Salman, 2017; Zhipeng et al., 2018). A VPN is a virtual encrypted tunnel between the user and a remote server operated by a VPN service. All external internet traffic is routed through this tunnel, making information safe from cybercriminals (Salman, 2017). Ali, Hossain, and Parvez (2015) pointed out that VPNs join networks of all sizes and eliminate the complexity of hardware and software required to segment networks.

Finally, Patel and Sistani (2018) differentiated between two distinct types of VPNs: Site-to-Site VPNs and Remote Access VPNs. The basic difference between the two is that remote access VPNs provide access using a mix of virtual circuits from a provider, as well as through the convenience of internet access, whereas site-to-site VPNs, while still using virtual circuits, limit accessibility to geographically dispersed offices of an organization. In today's computing environment, most organizations utilize home based or "teleworkers", so it is important to understand that virtual private networks can provide secure networks if an individual connects to one from home. VPNs are affordable options for secure computing to small companies and individuals.

SECURE VPN PROTOCOLS

Layer 2 Tunneling Protocol (L2TP) and IPsec

Puthal et al. (2017) pointed out that Transmission Control Protocol (TCP) and Internet Protocol (IP) are still the prevailing protocols for network communication involving private and public networks (i.e., the Internet). Since these protocols do not present security options, other protocols must be introduced to ensure confidentiality, authentication, and integrity.

Although separate protocols, L2TP and IPsec are usually discussed in a pair, since L2TP provides tunneling for VPNs, but no real security. IPsec provides network layer or IP address security, and can encrypt information about L2TP. As previously described, IP protocol, in its raw form, identifies the logical address associated with an interface (computer, router, storage device) connected to a network in clear text. IPsec provides data encryption at the network layer of the OSI Model.

L2TP

Yadav (2016) indicated that L2TP was developed in cooperation between Cisco and Microsoft. Layer 2 Tunneling Protocol provides physical and logical tunneling. This action creates a virtual path through various intranet and internet connections to create the effect of physical tunnel between network nodes. L2TP is used by Internet service providers (ISPs) to enable virtual private networks. L2TP is similar to the Data Link Layer Protocol in the OSI reference model, in that it connects physical devices as if they are in the same local area network. However since it uses authentication (log in), it actually more resembles a session layer protocol. (Salman, 2017).

A major advantage of L2TP is that it uses UDP (broadcast) ports, which frees it from the overhead of Transmission Control Protocol (TCP), and therefore is fast and efficient. L2TP becomes encrypted as service of IPsec, which we will discuss below. It provides a secure tunnel, reliable, scalable, fast, and flexible, is an established industry standard, and has the best authorization policy for users with VPN authentication. ("Layer 2 Tunneling", 2019). L2TP does not supply encryption or protection from the traffic that passes through the connection. (Salman, 2017; Zhiyong et al., 2013); this is supplied by IPsec.

Singh and Gupta (2016) pointed out that this tunneling protocol provides a first step in secure mode of transport. A VPN encapsulates the IP datagram into a tunneling protocol, thus hiding the original data from intruder or hackers. This establishes a point-to-point or multipoint link between the communicating parties in a public or shared communication network. Traditional VPNs uses DES (Data Encryption Standard), AES (Advance Encryption Standard), which uses 128 or 256 encryption bit algorithms, and are very secure. With IPsec encapsulation, the resultant message is further enclosed with an IPsec header. IPsec is designed to specify security in between communication channel of two communication devices, such as computers, gateways, routers and firewalls.

Jahan, Rahman, and Saha (2017) indicated that 63% of the companies uses site-to-site VPN to connect their branch offices, and 90% of the workers from home uses remote access VPN to communicate. For remote access, L2TP is

more preferable than other point-to-point protocol, especially applicable for the bandwidth, time, and security sensitive applications.

Advantages and Disadvantages of L2TP

Singh and Gupta (2016) discussed the advantages of L2TP to include the following: support for both IP and Non-IP networks and protocols; support of multiple tunnels; and compatibility with network address translation (NAT). NAT involves remapping IP protocols from public to private addresses to build firewall protection and save on IP address depletion. L2TP eliminates the network traffic by flow control mechanism to address congestion and keeps overhead to minimum. Disadvantages of L2TP include the fact that VPNs tunneling adds an overhead to IP packets size, that effects bandwidth utilization in network specifically if the data packet size is short (Salman, 2017).

IPsec

Often paired with L2TP, the Network Layer protocol IPsec offers data integrity, data confidentiality, and authentication of data. IPsec provides an end-to-end approach designed by IETF (Internet Engineering Task Force). It provides a bundle of protocols such as IPsec Key Exchange and Management Protocol (ISAKMP) for key management, which specifies the negotiation and establishment of security. Internet Key Exchange (IKE) is used for key exchange, which creates a secure channel to protect the negotiation in the set up the IPsec tunnel for traffic protection. Authentication Header (AH) offers authentication originality and integrity Encapsulated Security Payload (ESP) offers authentication originality, connectionless integrity, anti-replay service, and data confidentiality, to assure cryptography based security to the information that is transmitted over the network (Salman, 2017; Zhipeng et al., 2018).

Advantages and Disadvantages of IPsec

Patil and Korde (2018) indicated that IPsec has been criticized for its complexity with encryption key usage, and hash algorithms. Elezia and Raufia (2015) defended this complexity as a strength of the keys used, ensuring that there are no ways to bypass the security of the overall system. IPsec provides confidentiality by encrypting the data payload, integrity by calculating at each communicating endpoint the checksum or hash value of the data exchanged, and it provides authentication through signatures and certificates. IPsec protects against vulnerability to attacks like spoofing and session hijacking, IPsec can offer confidentiality, integrity, authentication services, as well as (optionally) by utilizing the Encapsulating Security Payload (ESP) and Authentication Header (AH) protocols (Geneiatakis et al., 2006; Sridevi, 2018). Gupta and Jha (2015) reported that IPsec may be vulnerable to login cracking. This attack involves recovering of Internet Protocol Security (IPsec) Pre-shared secret key (PSK) by using brute force attacks on VPN authentication protocols. The authors add that these attacks are easily discoverable and manageable.

Transport Layer Security Protocol (TLS)

TLS, and its predecessor secure socket layer (SSL), are the most common encryption protocols in use today. All HTTPS websites are protected with SSL/TLS (Patel & Sistani, 2018). Zhipeng et al. (2018) described TLS as VPN technology that works between the Layer 4 (Transport layer) and Layer 7 (Application layer) of OSI layers. To establish secure connection for communication between application tiers, TLS uses the certificate-based authentication, data encryption, and message integrity verification mechanisms. The use of SSL VPN is mostly in Web-based remote security access.

Patel and Sistani (2018) discussed how for authentication purposes, TLS uses an eight step Handshake protocol to establish the identity of a peer, using a combination of public and private keys to initiate encryption. Khan and Deshmukh (2014) stated that encryption with TLS helps prevent such exploits as man-in-the-middle (MITM), spoofed attacks, and session hijacking, using keys and hashing techniques. Ja (2019) described how TLS uses a Public key infrastructure (PKI) provides a solution for registering and managing a trustworthy public key. Government agencies or standard organizations manage registrar's keys. The authors point out that the most utilized application-layer protocol, the Hyper Text Transfer Protocol (HTTP), was designed without any security considerations. The popularity of HTTP and its wide adoption for ecommerce necessitated strict security requirements. A secure version called HTTPS was introduced by using security services from the transport layer, which allows the URL, content, forms and cookies to be encrypted during communication. Application using Secure HTTP (HTTPS) use TLS as a security protocol.

Advantages and Disadvantages of TLS

The primary advantage of TLS is that it is the most deployed encryption technique (Patel & Sistani, 2018). Ja (2019) pointed out that the current version and of TLS (1.3) has evolved due to issues with prior versions with attacks and vulnerabilities. This list of 15 attacks and their mitigation is described in RFC 7457.

The authors point out that many of these vulnerabilities are due to an improper implementation. For example, the TLS design problem of calculating media access control (physical) addresses before encryption results in a timing attack called the Lucky Thirteen attack, which allows attackers to decrypt text. In addition, the hop-by-hop (computer by computer) nature of TLS security is a major drawback, given that in every hop encryption/decryption is required (Geneiatakis et al. 2006; Sridevi, 2018). Stallings (2011) described how when two computers initiate a secure session, one computer creates a symmetric key and sends it to the other computer using public-key encryption. The two computers can then communicate using symmetric-key encryption. TLS provides confidentiality using symmetric encryption and message integrity using a message authentication code. This includes mechanisms to enable two TCP users to determine the security services they will use during the initial TLS handshake. For the ClientKeyExchange message, the client generates what is called the premaster secret, consisting of 48 bytes. This secret is sent to the server as part of this message, but is encrypted with the server's public key (obtained from the server's certificate) so that only the server can decrypt it with its private key (as messages are still being sent as plain text). This exchange prohibits hacking.

The Browser Exploit Against SSL/TLS (BEAST) attack exploits the predictable initialization TLS implementation due to use of the Cipher Block Chaining (CBC), allowing an attacker to decrypt parts of a packet. (Ja, 2019). Blackshaw (2015) described BEAST as a browser exploit against TLS that was revealed in late September 2011. This attack exploited weaknesses in cipher block chaining (CBC) in TLS. The CBC vulnerability can enable man-in-the-middle attacks against TLS in order to silently decrypt and obtain authentication tokens, thereby providing hackers access to data passed between a Web server and the Web browser accessing the server. It can be accomplished by sending Java script requests to a server and analyzing the encrypted server response to guess at the encryption algorithm.

Heartbleed is one of the most serious vulnerabilities ever found in TLS software, allowing the theft of server keys, user session IDs and user passwords from compromised systems. It was not, however, an SSL/TLS protocol flaw, but rather an implementation bug (known as a buffer over-read) The total cost of Heartbleed has been estimated to be in the range of hundreds of millions of dollars (Feilner, 2006; Skendzic & Kovacic, 2017).

OpenVPN

OpenVPN is an open-source, highly configurable, extremely popular VPN protocol for a variety of ports and encryption types (Feilner, 2006; Skendzic & Kovacic, 2017). OpenVPN deploys a modular concept for both security and networking. OpenVPN uses the SSL/TLS mechanisms for authentication and encryption, and does not suffer from the complexity that characterizes other VPN implementations like market leader IPsec (Feilner, 2006; Skendzic & Kovacic, 2017).

OpenVPN offers possibilities that are not offered in other VPN implementations. For example, OpenVPN offers two basic modes, which run either as Layer 2 or as Layer 3 VPN. OpenVPN tunnels can also transport Ethernet Frames, IPX packets, and Windows Network Browsing packets (NETBIOS), all of which are problems in most other VPN solutions. Once OpenVPN has established a tunnel, the central firewall in the company's central branch can protect any laptop, even if it is not a local machine. Any employee can protected by the central firewall whenever connected. OpenVPN can be configured to run as a TCP or UDP service, and as server or client. All firewall rules, restrictions, forwarding mechanisms, and concepts like NAT can be used with OpenVPN.

Installation is reputed to be simple, when compared to IPsec**.** Applications use the encryption libraries, algorithms, key exchange, and digital certificates of SSL/TLS with UDP or optional TCP packets (Feilner, 2006; Skendzic & Kovacic, 2017).

Advantages and Disadvantages of OpenVPN

As far as advantages, OpenVPN enables secure user authentication using a public (static) key, and user names and passwords. The firewall options and flexibility of vendors' protocol suites have been discussed.

As far as weakness, OpenVPN is not IPsec compatible, and IPsec is the standard VPN solution. Many popular network devices, such as Cisco or Bintec routers, use IPsec and can connect to applications of other manufacturers or software IPsec clients. Although OpenVPN can be simple to implement, industry knowledge of this protocol, which was introduced in 2001, is somewhat limited. With respect to disadvantages, it should be noted that OpenVPN is not a multi-thread application, which limits its rate of operating network connections (approximately up to 100 connections). In case more connections are needed, additional processes, different ports or IP addresses need to be deployed (Skendzic & Kovacic, 2017).

RESULTS

The evolution of virtual private networks secure protocols continues to develop, and offer choices for low cost connections, telecommuting, and ubiquitous security. Whether organizations deploy their own virtual private network, or use vendors, there are several options. Along with modifications and upgrades to secure protocols such as L2TP, IPsec, TLS, and OpenVPN, we have discussed advantages and limitations, as well history of security breaches, in an effort to evaluate the protocols.

Research question #1: is there a preferred choice of protocols for implementation in a virtual private network as evaluated in the context of the Open Systems Interface?

To begin with, this is not an assessment of the functionally of the protocol, installation, maintenance, and performance, rather it is an analysis of strength of network defense. It begins with analysis with respect to the OSI Model. All of the protocols reviewed provide security solutions, and are production in production network environments.

The protocols IPsec and OpenVPN both operate at Layer 3 of the model, the lowest level of the sample of protocols that have been examined here. TLS operates at Layer 4 of the OSI Model. See Table 1: Map of Secure Protocols to the OSI Model (above).

However, IPsec cannot provide physical and logical tunneling, a requirement for virtual private networks. It relies on L2TP protocol to perform this. L2TP requires authentication/login, so is operating a Layer 5 of the OSI Model, and does not provide machine level security. This makes OpenVPN a clear choice on this dimension.

In addition, a single protocol, OpenVPN, that can provide the same layer of protection as an alternative with two protocols, will require less overhead than a two-protocol solution. Furthermore, OpenVPN allows configuration of the TCP port that it uses to tunnel to applications, whereas IPsec does not (Hoffman, 2018). For these reasons, OpenVPN would be the clear protocol of choice. Since OpenVPN and L2TP/IPsec are not compatible, vigilance is needed to assess the implementation of these protocols in a new or existing virtual private network.

SUMMARY AND FUTURE CONSIDERATIONS

Many commercial analysts espouse the virtues of OpenVPN (Bishchoff, 2019; Hoffman, 2018). However, the landscape continues to change, as scientists today are embracing new protocol development. For example, WireGuard was recently proposed as a replacement for existing secure communications protocols like IPsec and OpenVPN. It has numerous benefits, including its simplicity and ease of configuration, high performance software, and small codebase, making it relatively easy to audit compared to large, complex code bases typically encountered with other protocols (Donenfeld, 2017; Dowling & Paterson 2018; Lipp et al., 2019).

Stallings (2011) commented that virtually all businesses, most government agencies, and many individuals now have websites, and the proliferation of the Internet for electronic commerce continues to be rapid. However, as we have seen, the vulnerability of insecure web sites can pose significant problems, even in the largest companies.As we commonly use credit cards for e-commerce activity, the threat of stolen information is tangible for everyone.

Airehrour, Gutierrez, and Ray (2016) pointed to the propagation of the Internet of Things, which promises to connect billions of connected devices, including cars, mobile phones, and household devices and entry systems. The Internet

of Things also holds the promise for more successful management of hospitals, smart grids, and smart buildings (Kumar, Vealey, & Srivastava, 2016; Soceanu, Vasylenko, & Gradinaru, 2017). Security is fundamental to the success deployment of the IoT. Network professional and students of networks need to be proficient in the evaluation and deployment of secure network protocols to make a secure IoT. For example, evaluators and implementers of secure protocols must understand the consequences of decommissioning of TLS and IPsec, when considering the implementation of OpenVPN. Vendors are available to help, but small to medium size companies need to understand the working of the protocols to make or implement informed choices in their security strategies.

REFERENCES

Airehrour, D., Gutierrez, J., & Ray, S. (2016). Secure routing for internet of things: a survey. *Journal of Network and Computer Applications, 66,* 198–213.

Ali, M., Hossain, M. & Parvez, M. (2015). Design and Implementation of a Secure Campus Network. *International Journal of Emerging Technology and Advanced Engineering, 5*(7), 370-374.

American Express, IBM Sign $4B Deal. (2002, February 25). Retrieved from https://www.informationweek.com/american-express-ibm-sign-$4b-deal/d/d-id/1013884

American Express, IBM Set Technology Outsourcing Deal. (2002, February 25). Retrieved from https://www.wsj.com/articles/SB1014656709248066360

Bishchoff, P. (2019, February 2). VPN protocols explained and compared. Retrieved from https://www.comparitech.com/vpn/protocols/

Blackshaw, B. (2015). *Secure Network Protocols. How SSL/TLS, SSH, SFTP and FTPS work*. Yeronga, Australia: Enterprise Distributed Technology Pty Ltd.

Cirincione G., Pham, T., Ladas, A., Stanton, B., & Fisher, G. (2019, May 10). Design and implementation of the U.S. Army Artificial Intelligence Innovation Institute, Proc. SPIE 11006, Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications. Retrieved from https://doi.org/10.1117/12.2524026

Donenfeld. J. (2017). *WireGuard: Next Generation Kernel Network Tunnel.* Proceedings of the 2017 Network and Distributed System Security Symposium. San Diego, CA, Feb. 26 - March 6, 2017, 1-17.

Dowling, B., & Paterson, K. (2018). A cryptographic analysis of the WireGuard protocol. Retrieved from https://eprint.iacr.org/2018/080.

Elezia, M. & Raufia, B. (2015). Conception of Virtual Private Networks using IPsec suite of protocols, comparative analysis of distributed database queries using different IPsec modes of encryption. *Procedia - Social and Behavioral Sciences, 195,* 1938 – 1948.

Feilner, M. (2006). *OpenVPN: Building and Integrating Virtual Private Networks*. Birmingham UK: PACKT Publishing.

Frank, M. (2017). *Introduction to networks v6: Companion guide*. Indianapolis, IN: Cisco Press.

Garge, K. & Hegde, M. (2011). *Network security.* New Delhi: Barry Art Press.

Geneiatakis, D., Dagiuklas, T., Kambourakis, G., Lambrinoudakis, G., Gritzalis, S., Karlovassi, S., & Sisalem, D. (2006). Survey of security vulnerabilities in session initiation protocol. *IEEE Communications Surveys*, 8(3), 69-81.

Gupta, A. & Jha, R. (2015). *Security Threats of Wireless Networks: A Survey*. Paper presented at International Conference on Computing, Communication and Automation. Greater Noida, India, May 15 - 16, 2015.

Hoffman, C. (2018, April 4). Which is the Best VPN Protocol? PPTP vs. OpenVPN vs. L2TP/IPsec vs. SSTP. Retrieved from https://www.howtogeek.com/211329/which-is-the-best-vpn-protocol-pptp-vs.-openvpn-vs.-l2tpIPsec-vs.-sstp/.

Ja, S. (2019). *CyBOK Network Security Knowledge Area Issue 1*. London: National Cyber Security Centre.

Jahan, S., Rahman, M., & Saha, S. (2017). *Application specific tunneling protocol selection for virtual private networks*. Paper presented at the 11 International Conference of Networks, Systems, and Security. Helsinki, August 21–23, 2017, 39-44.

Jyothi, K. & Reddy, B. (2018). Study on Virtual Private Network (VPN), VPN's protocols and security. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 3*(5), 919-932.

Khan, S. & Deshmukh, S. (2014). Security in Cloud Computing Using Cryptographic Algorithms. *International Journal of Computer Science and Mobile Computing, 3*(9), 517-525.

Koujalagi, A. (2018). Network Security Intelligence for Small and Medium Scale Industry 4.0: Design and Implementation**.** *Global Journal of Computer Science and Technology, 18*(4), 1-11.

Kumar, S., Vealey, T., & Srivastava, H. (2016). *Security in Internet of Things: Challenges, Solutions and Future Directions.* Paper presented at 49th Hawaii International Conference on System Sciences. Manoa, Hawaii, June 5-8, 2016.

Layer 2 Tunneling Protocol (L2TP). (2019, May 5). Retrieved online from https://www.techopedia.com/definition/26196/layer-2-tunneling-protocol-l2tp

Lee, H., Lee, S., Seong, J., Rou, H., & Gim, G. (2019). A technical study of remote backup center performance using public virtual private network .vpn for data center back up. *International Journal of Advanced Computer Research, 9(*40), 1-10.

Lipp, B., Blanchet, B. & Bhargavan, K. (2019) *A Mechanised Cryptographic Proof of the WireGuard Virtual Private Network Protocol.* Paper to be presented at the Fourth IEEE European Symposium on Security and Privacy. Stockholm, Sweden, June 17 – 19, 2019.

Mazzarol, T. (2015). SMEs engagement with e-commerce, e-business and e-marketing. *Small Enterprise Research*, 22(1), 79-90.

Northcutt, S., Zeltser, L., Winters, S., Kent, K., & Ritchey, R.W. (2003). *Network Perimeter Security*. Indianapolis: New Riders.

Pandey, R. & Misra, M. (2016). *Cyber security threats—Smart grid infrastructure*. Paper presented at the 2016 National Power Systems Conference (NPSC). Bhubaneswar, India, December 19 -21, 2016.

Patel, A. & Sistani, A. (2018). Design and Evaluation of a virtual private network architecture for collaborating specialist users. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 3*(5), 2456-3307.

Patil, V. & Korde, S. (2018). Protocols for Virtual Private Networks. *International Journal of Emerging Technology and Computer Science, 3*(4), 16-22.

Puthal, D., Mohanty, S., Nanda, P. & Choppali, U. (2017). Building Security Perimeters to Protect Network Systems against Cyberthreats. *IEEE Consumer Electronics Magazine*, 14-27.

Salman, F. (2017). Implementation of IPsec-VPN Tunneling using GNS3. *Indonesian Journal of Electrical Engineering and Computer Science, 7*(30), 885-860.

Singer, P., & Friedman, A. (2014). *Cybersecurity and Cyberwar*. New York: Oxford University Press.

Singh, K. & Gupta, H. (2016). *A New Approach for the security of VPN*. Proceedings of the Second International conference on Information and Communication Technology for Competitive Strategies, Udaipur, India, March 4 - 5, 2016.

Skendzic, A. & Kovacic, B. (2017). Open source system OpenVPN in a function of Virtual Private Network. *Asia-Pacific Journal of Information Technology and Multimedia, 5(*1), 15 – 30.

Soceanu, A., Vasylenko, M. & Gradinaru, A. (2017). *Improving Cybersecurity Skills Using Network Security Virtual Labs.* Proceedings of the International MultiConference of Engineers and Computer Scientists. Hong Kong. March 15 - 17, 2017.

Sridevi, C. (2018). A Survey of Network Security. *Global Journal of Computer Science and Technology, 17*(5), 29-34.

Stallings, W. (2011). *Network security essentials: applications and standards 4th ed.* Upper Saddle River, NJ: Prentice Hall.

Vachon, R., & Graziani, R. (2008). *Accessing the WAN, CCNA Exploration Companion Guide*. Indianapolis, IN: Cisco Press.

Yadav, A. (2016). Security Structure of VPN. A Survey. *International Journal of Recent Innovation in Engineering and Research (1)*1, 19-24.

Zameer, A, Pandow, B.A. & Singh B. (2017). *Economic hurdle for implementation of cloud computing in higher education in Sultanate of Oman*. Paper presented at Infocom Technologies and Unmanned Systems (Trends and Future Directions). Dubai, United Arab Emirates, December 18-20, 2017.

Zhipeng, Z, Chandel, S., Jingyao, J., Shilin, Y., Yunnan, Y., & Zang, J. (2018). *A Comparative Study of MPLS, IPsec, and SSL Virtual Private Networks.* Proceedings of the Second International Conference on Computing Methodologies and Communication. Rayapalayam, India, February 16-18, 2018.

Zhiyong, L., Guixin, Y., & Hongzhuo, Q. (2013). *Research of A VPN Secure Networking model.* Proceedings of 2013 2nd International Conference on Measurement, Information and Control. Harbin, China, 567-569.